

Smart 116 IP

User Guide



www.minicom.com

International HQ

Jerusalem, Israel

Tel: + 972 2 535 9666

minicom@minicom.com

North American HQ

Linden, NJ, USA

Tel: + 1 908 486 2100

info.usa@minicom.com

European HQ

Dübendorf, Switzerland

Tel: + 41 44 823 8000

info.europe@minicom.com

Technical support - support@minicom.com

Table of Contents

1. Welcome	4
Section I	5
2. Introduction	5
3. Key features	5
4. System components.....	6
5. Compatibility	6
6. Terminology	6
7. The Smart 116 IP unit	6
7.1 LED and button table	7
7.2 Connector table	7
8. Pre-installation guidelines.....	7
8.1 Avoiding general rack mounting problems	8
8.2 Rack mounting the Smart 116 IP	8
9. Client computer operating system.....	9
10. Connecting the system.....	9
10.1 Connecting to the network	10
10.2 The RoC/RICCs	10
10.2.1 Connecting a RoC/RICC PS/2	11
10.2.2 Connecting a RoC/RICC USB	12
10.2.3 Connecting a RICC SUN	12
10.3 Connecting the CAT5 cables	13
10.4 Connecting a KVM console	13
10.5 Connecting the power supply	13
11. Initial settings - Default IP address	13
11.1 Static IP addresses for a number of units	13
12. Logging into the Web interface	14
12.1 SSL Certificate notes	15
13. Network > Configuration	15
13.1 LAN 1	15
13.2 KVM.net	15
14. Saving changes	16
15. Administration > User Settings	16
15.1 Adding a user	17
15.2 Editing a user	17
15.3 Deleting a user	18
15.4 Blocking a user	18
16. Administration > Switch Configuration.....	18
17. Administration > User Targets	19
18. Security > Settings	20
19. Security > SSL Certificate	21
20. Maintenance > Firmware Upgrade.....	21
21. Restore Factory Settings.....	22

22. Logging out	22
23. Starting a remote session	23
23.1 Taking over a busy remote session.....	24
23.2 Full screen mode.....	24
23.3 The Toolbar	25
23.4 Switching to a different server	25
23.5 Changing the performance settings	25
23.6 Adjusting the Video settings	26
23.6.1 Refresh.....	27
23.6.2 Manual Video Adjust.....	27
23.6.3 Auto Video Adjust	28
23.7 Power cycle	28
23.8 Keyboard key sequences	28
23.9 Synchronizing mouse pointers	30
23.9.1 Aligning the mice pointers	30
23.9.2 Calibrating mice pointers	30
23.9.3 Manual mice synchronization	30
23.10 Minicom icon menu features.....	32
23.11 Disconnecting the remote session	33
24. Troubleshooting - Safe mode.....	33
24.1 Entering Safe mode	33
24.2 Restoring factory defaults	34
24.3 Restoring the device firmware	35
Section II	36
25. Switching between computers	36
25.1 The keyboard hotkeys.....	36
26. The OSD.....	36
26.1 Navigating the OSD	37
26.2 Selecting a computer	37
26.3 The OSD settings - F2	37
26.3.1 The General settings	37
26.4 F7 Defaults	40
26.5 The Ports settings	40
26.5.1 Editing the computer name	40
26.5.2 Keyboard (KB)	41
26.5.3 Adding/changing a hotkey (HKEY)	41
26.6 The Time settings.....	41
26.6.1 Scan (SCN) - Label (LBL) - Time out (T/O)	42
26.7 Users	42
26.8 Security.....	43
26.9 The OSD HELP window – F1	44
26.10 Scanning computers – F4.....	45
26.11 Tuning – F5.....	45
26.12 Moving the label – F6.....	45
27. Upgrading the Smart 116 IP firmware	46
27.1 System requirements for the Update software	46
27.2 Connecting the Smart 116 IP System	46
27.3 Connecting the RS232 Download cable	46
27.4 Installing the software	47

27.5 Starting and configuring the Update software.....	47
27.6 Verifying the version numbers	49
27.6.1 116 IP Switch version	49
27.6.2 RoC/RICC version number.....	50
27.7 Obtaining new firmware	50
27.7.1 Updating the firmware	50
28. Update software - Troubleshooting.....	51
28.1 Resetting the Smart 116 IP or RoC/RICCs.....	51
28.2 Setting default values for the OSD	52
28.3 Get Status	52
28.4 Communication Error message	52
28.5 Electricity failure	52
29. Technical specifications.....	53
30. Video resolution and refresh rates.....	54
31. Safety.....	54
32. User guide feedback.....	54

© 2007 Copyright Minicom Advanced Systems. All rights reserved.

1. Welcome

Thank you for buying the Smart 116 IP system. This system is produced by Minicom Advanced Systems Limited.

This document provides installation and operation instructions for Minicom's Smart 116 IP. It is intended for system administrators and network managers, and assumes that readers have a general understanding of networks, hardware and software.

Technical precautions

This equipment generates radio frequency energy and if not installed in accordance with the manufacturer's instructions, may cause radio frequency interference.

This equipment complies with Part 15, Subpart J of the FCC rules for a Class A computing device. This equipment also complies with the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of the Canadian Department of Communications. These above rules are designed to provide reasonable protection against such interference when operating the equipment in a commercial environment. If operation of this equipment in a residential area causes radio frequency interference, the user, and not Minicom Advanced Systems Limited, will be responsible.

Changes or modifications made to this equipment not expressly approved by Minicom Advanced Systems Limited could void the user's authority to operate the equipment.

Minicom Advanced Systems Limited assumes no responsibility for any errors that appear in this document. Information in this document is subject to change without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Minicom Advanced Systems Limited.

Trademarks

All trademarks and registered trademarks are the property of their respective owners.

Section I

This section explains how to configure and operate the Smart 116 IP system remotely over IP.

Section II on page 36, explains how to operate the Smart 16 IP Switching system locally through the On Screen Display (OSD).

2. Introduction

The Smart 116 IP extends your KVM (keyboard, video, mouse) from any computer or server over TCP/IP via LAN, WAN or Internet connection. Now you can control, monitor and manage up to 16 remote servers from wherever you are, inside or outside the organization. The Smart 116 IP is a cost-effective hardware solution, for secure remote KVM access & control of 16 computers/servers from the BIOS level - independent of the OS. One local analog or one remote digital IP user can access and control 16 multi-platforms (PS/2, SUN, USB) servers at a time.

The Smart 116 IP is based on Minicom's innovative RoC technology in which each computer/ server is directly connected to the switch via RIC on Cable (RoC) using only standard CAT5 cable at a distance of up to 10m/33ft in a star configuration. No external power is needed at the remote RoC.

3. Key features

BIOS level control to any server's brand and model, regardless of the server condition and network connectivity, covering the entire spectrum of crash scenarios.

Compatible with all major operating systems. Supports many hardware and software configurations for the remote client and the target server computers, as well as the KVM switch in use.

Web-based control - Browser Control to a target server, from any location via secured standard IP connection.

Multi-user view mode - Allows simultaneous users to view remote sessions. Remote control can be intuitively handed between users with appropriate permissions.

Security - Supports the highest security standards for encryption (128 bit SSL and HTTPS) and authentication for remote user and advanced OSD management with multi-layer security for local user.

KVM.net - Can be controlled by the Minicom's KVM.net system for centralized over-IP management of distributed data center locations.

4. System components

The Smart 116 IP system consists of:

- 1 Smart 116 IP (p/n 1SU60005/R)
- Rack mounting set (p/n 5AC20247)
- 1 RS232 Download cable (p/n 5CB40419)
- 1 RS232 Cross cable (p/n 5CB00566)
- Remote Interface Connection cables (RICCs) – PS/2, SUN, USB
- RICC on Cable (RoCs) - PS/2, USB (SUN)
- CAT5 cables (1.5m provided)
- Rack mounts for the RICCs

5. Compatibility

The Smart 116 IP is compatible with:

- PS/2, SUN and USB computers/servers
- VGA, SVGA, or XGA monitors
- Windows, Linux, UNIX and other major operating systems

6. Terminology

Below are some terms and their meanings used in this guide.

Term	Meaning
Target server	The computers/servers that are accessed remotely via the Smart 116 IP.
Client computer	The PC running a remote Smart 116 IP session
Remote session	The process of remotely accessing and controlling Target Servers connected to Smart 116 IP from a user workstation

7. The Smart 116 IP unit

Figure 1 illustrates the front panel of the Smart 116 IP.

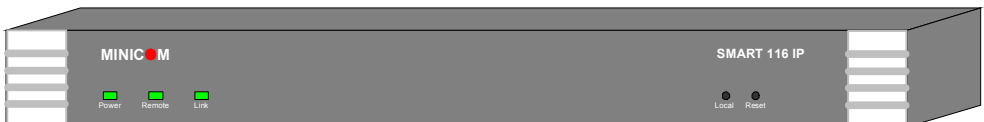


Figure 1 Smart 116 IP ports – side 1

7.1 LED and button table

LED	Function
Power	Power Indicator
Remote	Illuminates when remote session is active
Link	Unit is connected to the system
Button	Function
Local	When pressed, Smart 116 IP disconnects the Client computer's link to the Target Server and the local mouse and keyboard become operational. The Remote LED turns off.
Reset	Press and hold for more than 7 seconds to reset the Smart 116 IP unit

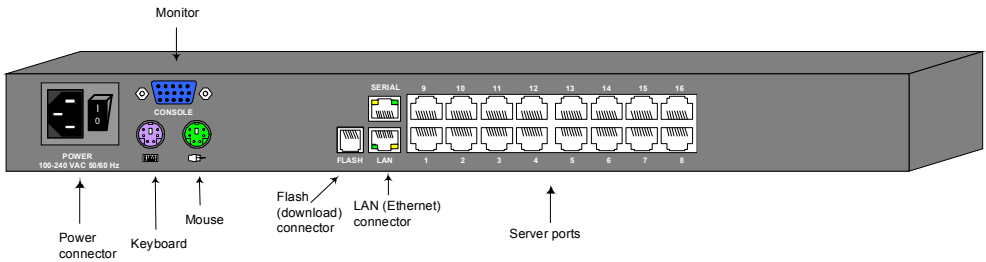


Figure 2 Smart 116 IP ports – side 2

7.2 Connector table

Connector	Function
Console KVM	(Optional) Connect a keyboard, video and mouse to operate the Smart 116 IP locally
Serial	This port is for future Serial functionality
Flash	To update firmware of the analogue part of the Smart 116 IP system - OSD, Switch, RICCs and RoCs.
LAN	Connect to 10/100 Mbit Ethernet. Yellow Led illuminates when connected to LAN. Green LED illuminates when a remote session is in progress
Server ports	Connect to servers via RoC/RICCs

8. Pre-installation guidelines

- Place cables away from fluorescent lights, air conditioners, and machines that are likely to generate electrical noise

- Place the Smart 116 IP on a flat, clean and dry surface
- The Smart 116 IP is not intended for connection to exposed outdoor lines
- Ensure that the maximum distance between each computer and the Smart 116 IP, does not exceed 10m/33ft

8.1 Avoiding general rack mounting problems

Elevated operating ambient temperature

The operating ambient temperature of the rack environment may be greater than the room ambient when installing into a closed or multi-unit rack assembly. So install the equipment in an environment compatible with the maximum rated ambient temperature.

Reduced airflow

Install the equipment in a rack in such a way that the amount of airflow required for safe operation is not compromised. Leave a gap of at least 5cm/2” each side of the Smart 116 IP.

Mechanical loading

Mount the equipment in the rack in such a way that a hazardous condition is not achieved due to uneven mechanical loading.

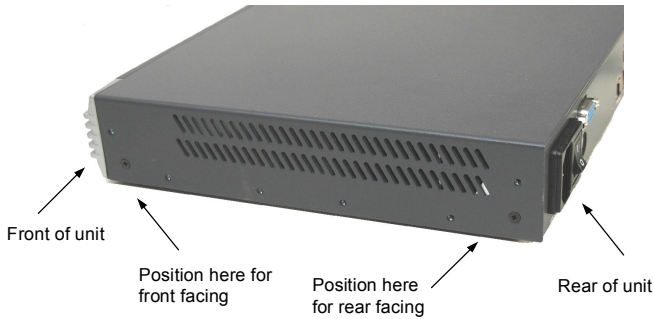
Circuit overloading

When connecting the equipment to the supply circuit, consider the effect that overloading of circuits might have on over-current protection and supply wiring.

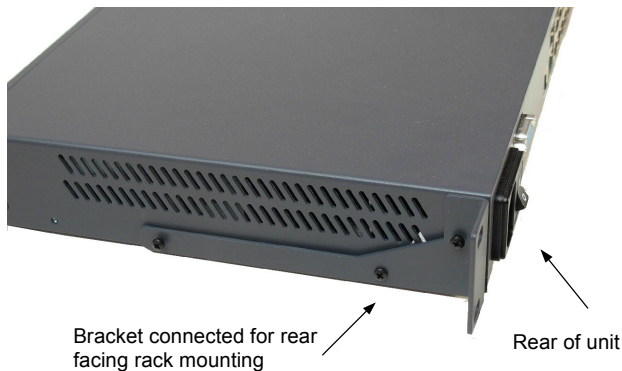
Reliable earthing of rack-mounted equipment should be maintained. Give attention to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

8.2 Rack mounting the Smart 116 IP

Rack mount the Smart 116 IP using the supplied Rack-mount kit. The brackets can be placed in 2 possible positions, see Figure 3.

**Figure 3**

Place the brackets towards the front of the unit so that the unit can be mounted front facing, or place the brackets towards the rear of the unit so that the unit can be mounted rear facing. Figure 4 illustrates the bracket connected for rear facing. Screw the bracket to the Smart 116 IP using the screws provided.

**Figure 4**

9. Client computer operating system

Windows 2000 or higher, with Internet Explorer 6.0 or later version. 128 bit encryption support is required.

10. Connecting the system

Figure 5 illustrates the Smart 116 IP system overview.

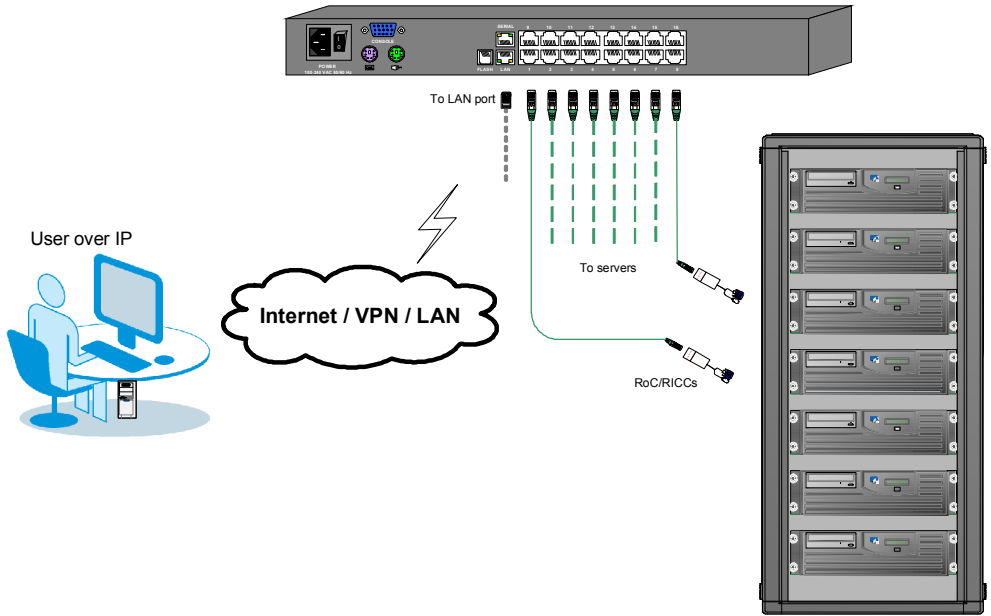


Figure 5 Smart 116 IP system overview

10.1 Connecting to the network

Connect the network cable to the LAN port of the Smart 116 IP. This must be done before powering on the Smart 116 IP.

10.2 The RoC/RICCs

Each computer/ server is directly connected to the Smart 116 IP via the appropriate RoC or RICC using CAT5 cable in a star configuration. No external power is needed at the remote RoC/RICCs. The RoC/RICCs draw their power from the computer's keyboard port (RoC/RICC PS/2, SUN) or from the USB port (RoC/RICC USB). The figures below illustrate the RoC PS/2 and RoC USB.

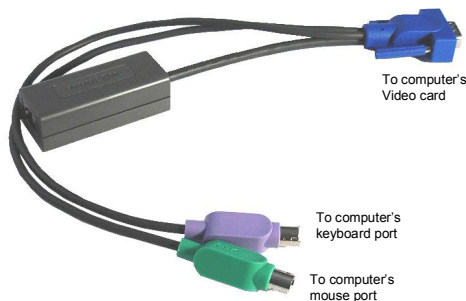


Figure 6 RoC PS/2

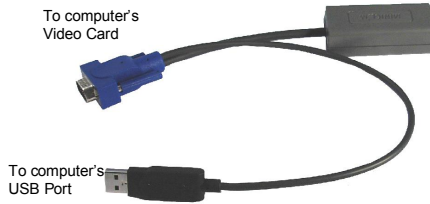


Figure 7 RoC USB (SUN)

10.2.1 Connecting a RoC/RICC PS/2

The connections for RoC/RICC PS/2 are exactly the same. Figure 8 illustrates the RICC PS/2.

You can connect the RoC/RICC PS/2 to a powered on computer, but it must be in the following order:

1. Connect the Mouse connector to the computer's Mouse port.
2. Connect the Keyboard connector to the computer's Keyboard port.
3. Connect the Screen connector to the computer's Video port.

Failure to connect in the above order while the server is running, may lead to the mouse malfunctioning until the server is rebooted.

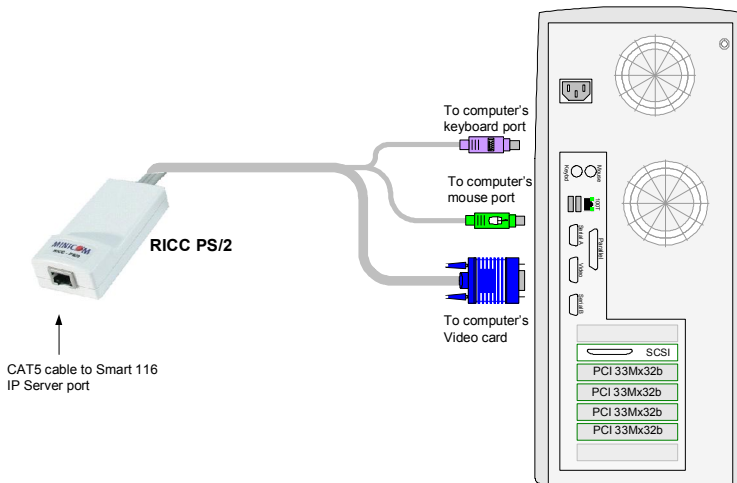


Figure 8 RICC PS/2 connections

10.2.2 Connecting a RoC/RICC USB

The RoC/RICC USB supports Windows 98 SE and later, MAC, SUN and SGI, and all modern Linux distributions. The connections for RoC/RICC USB are exactly the same. Figure 9 illustrates the RICC USB and its connections.

To connect the RoC/RICC USB:

1. Connect the Screen connector to the computer's Video port.
2. Connect the USB connector to the computer's USB port.

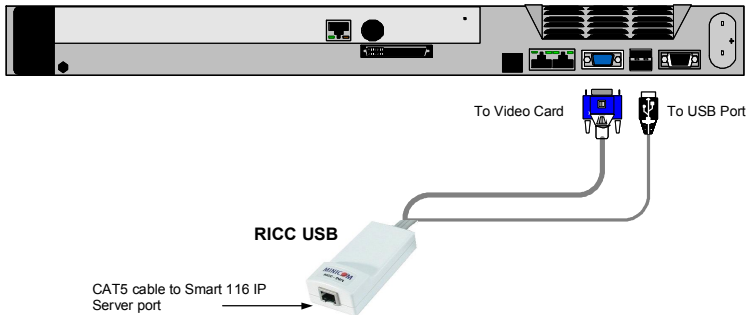


Figure 9 RICC USB

10.2.3 Connecting a RICC SUN

Figure 10 illustrates the RICC SUN and its connections.

To connect the RICC SUN:

1. Connect the Screen connector to the computer's Video card.
2. Connect the Keyboard connector to the computer's Keyboard port.

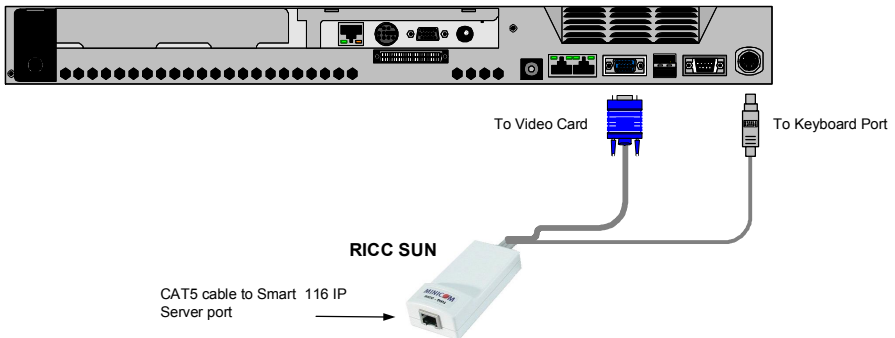


Figure 10 RICC SUN

10.3 Connecting the CAT5 cables

1. Connect one connector to the RoC/RICCs RJ45 port.
2. Connect the other connector to one of the Smart 116 IP's Computer ports.
3. Follow the above 2 steps for each computer.

10.4 Connecting a KVM console

To operate the system locally, connect a KVM console to the Smart 116 IP:

1. Connect the monitor's connector to the Smart 116 IP's Monitor port.
2. Connect the keyboard's connector to the Smart 116 IP's Keyboard port.
3. Connect the mouse's connector to the Smart 116 IP's Mouse port.

10.5 Connecting the power supply

1. Connect the Smart 116 IP to the power supply using the Power cord provided. Only use the power cord supplied with the unit.
2. Switch on the servers/computers.

11. Initial settings - Default IP address

The following sections provide instructions for setting the IP address for the Smart 116 IP unit.

By default, Smart 116 IP boots with an automatically assigned IP address from a DHCP (Dynamic Host Configuration Protocol) server on the network. The DHCP server provides a valid IP address, gateway address and subnet mask.

To identify the IP address, the Smart 116 IP MAC address appears on the underside of the Smart 116 IP box. The device number (D.N.) can also be found there.

If no DHCP server is found on the network, Smart 116 IP boots with the static IP address: 192.168.0.155.

Note! If a DHCP server later becomes available, the unit picks up the IP settings from DHCP server. To keep the static IP address, disable DHCP – explained in section 13.1 on page 15.

11.1 Static IP addresses for a number of units

Where you want to connect more than 1 Smart 116 IP to the same network and there is no DHCP server, or you want to use static IP addresses, do the following:

Connect the Smart 116 IP units one at a time and change the static IP address of each unit before connecting the next unit.

12. Logging into the Web interface

Complete the initial setup via the Web configuration interface:

1. Open your Web browser (Internet Explorer version 6.0 or higher).
2. Type the Smart 116 IP system IP address - `https://IP address/config` - and press **Enter**. The login page appears, see Figure 11.

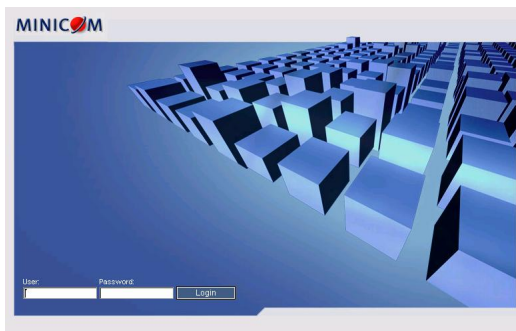


Figure 11 Login page

3. Type the default Administrator user name - **admin** - and password - **access** - (both lower case).
4. Press **Enter**. The Web interface opens at the Network Configuration page. See Figure 12.
5. Bookmark the page for easy reference.



Figure 12 Smart 116 IP Web interface

12.1 SSL Certificate notes

When first connecting to Smart 116 IP's https configuration page, 2 browser security warnings appear. Click **Yes** to proceed.

The first warning disappears upon first Smart 116 IP client installation, when Minicom's root certificate is installed.

13. Network > Configuration

Consult your Network Administrator for the network settings.

Device name - Type a name for the Smart 116 IP. Default device name consists of the letter 'D' followed by the 6-digit device number (D.N.) found on the silver label on the underside of the Smart 116 IP box.

First TCP Port - Choose 3 consecutive ports, and type in the first port number of the series. The default port – 900 – is suitable for the majority of installations.

Note

Firewall or router security access list must enable inbound communication through the selected TCP ports for the Smart 116 IP's IP address.

For Client computer access from a secured LAN, the selected ports should be open for outbound communication.

13.1 LAN 1

Under LAN 1 in Figure 12, is the following:

Enable DHCP – When a DHCP server is active on the same network to which Smart 116 IP is connected, DHCP provides automatic IP assignment.

When DHCP is disabled – (Recommended) – You can assign a fixed IP address to the Smart 116 IP.

Consult your Network Administrator regarding the use of the DHCP. **Note!** Where you have access to the server – your configured (or default) Smart 116 IP device name will appear on the DHCP server's interface, making it easy to locate.

When DHCP is disabled, enter the **IP Address**, **Subnet Mask**, and **Default Gateway** for **LAN 1**, as given by your Network Administrator.

13.2 KVM.net

KVM.net is a centralized IP based system for secure control of servers and network devices, power and user administration in the data center environment. KVM.net combines Out-Of-Band, KVM via IP access with modern IT standards and

requirements. It is the most comprehensive remote server maintenance solution available in the market today.

Enable KVM.net - Check this option to allow Smart 116 IP unit to be remotely managed by Minicom's KVM.net system.

Manager Auto Discovery – when checked, KVM.net automatically detects the Smart 116 IP, if it resides on the same network segment.

Manager IP – If Smart 116 IP resides on a different segment, type the static IP address of the Smart 116 IP.

14. Saving changes

Click **Save & Restart** to save any configuration changes and restart the Smart 116 IP system.

15. Administration > User Settings

From the menu click **User Settings**, Figure 13 appears.

User Name	Permission	Status
1. Spock	Administrator	
2. view	View Only	
3. user	User	
4. admin	Administrator	

Figure 13 User Settings

On this page an Administrator creates and edits users.

There are 3 levels of user access:

- Administrator
- User
- View only

Administrator

An Administrator has unrestricted access to all windows and settings and can “take over” any active session (explained in section 23.1 on page 24). An Administrator can change the name and password and Target server permissions of all users.

User

A User can access/control Target Servers, but cannot use the advanced mouse settings.



A User has no access to the Web configuration interface.

View only

View only can view the screen of the currently accessed Target Server without keyboard and mouse control. A “view only” indicator appears on the viewer’s local mouse pointer.



15.1 Adding a user

To add a user:

1. Click  and type a name and a password. The password must be at least 6 characters – letters or numbers, and must not include the user name, even if other characters are added. Depending on the security level chosen the user name and password parameters are different. See section 18 on page 20.
2. Select the permission type from the **Permission** box.
3. Click , the user appears in the list of users.



15.2 Editing a user

To edit a user:

1. Select the user from the list.
2. Click . You can now change all the parameters – user name, permission and password.
3. Click , the changes are saved.

15.3 Deleting a user

To delete a user:

1. Select the user from the list.
2. Click .
3. Click , the changes are saved.

15.4 Blocking a user

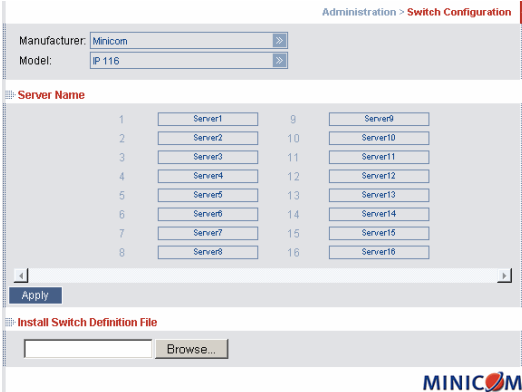
An alternative to deleting a user is blocking a user. This means that the user's name and password is stored, but the user is unable to access the system. Check **Block** to block a user. Uncheck **Block** to allow the user access.

16. Administration > Switch Configuration

Give the servers connected to the Smart 116 IP unique names, so that users accessing the system can identify the servers easily.

To do so:

1. From the menu click **Switch Configuration**. The Switch Configuration window appears, see Figure 14.



Administration > Switch Configuration

Manufacturer:

Model:


Server Name

1	<input type="text" value="Server1"/>	9	<input type="text" value="Server9"/>
2	<input type="text" value="Server2"/>	10	<input type="text" value="Server10"/>
3	<input type="text" value="Server3"/>	11	<input type="text" value="Server11"/>
4	<input type="text" value="Server4"/>	12	<input type="text" value="Server12"/>
5	<input type="text" value="Server5"/>	13	<input type="text" value="Server13"/>
6	<input type="text" value="Server6"/>	14	<input type="text" value="Server14"/>
7	<input type="text" value="Server7"/>	15	<input type="text" value="Server15"/>
8	<input type="text" value="Server8"/>	16	<input type="text" value="Server16"/>

Install Switch Definition File

MINICOM

Figure 14 Switch Configuration

2. In the **Server Name** section change the name of the connected servers by selecting the server name and typing a new name. Click  to save changes.

Install switch definition file

In the event that Minicom's Technical Support updates the Switch Definition file, the file will be available in the Support section of our website - www.minicom.com.

1. Load the file onto the Client computer.
2. Locate and install the Switch Definition file. The switch definition file is replaced.

17. Administration > User Targets

By default access is denied to all servers for all user types including Administrators. You must define the access rights of each user separately.

To do so:

1. From the menu click **User Targets**. The User Targets Configuration window appears, see Figure 15.



Figure 15 User Targets Configuration

2. Select a user from the User drop-down menu.
3. Check the Target servers the user can access (according to his access permissions). To select all Target servers, press Select All.
4. Click Apply, the selection is saved.
5. Repeat the above steps for each user.

18. Security > Settings

Configure the security features, such as Account Blocking, Password Policy and Idle Timeout, as explained below.

From the **Security** section click **Settings**, the **Security Settings** appear, see Figure 16.

The screenshot shows the 'Security > Settings' configuration page. It is divided into three main sections:

- Account Blocking:** Includes a 'Block after' field set to 3 attempts within H 0 M 1. Below it, 'Block account for' is set to H 0 M 3, with an unchecked checkbox for 'forever'.
- Password Policy:** Features a checkbox for 'High security password policy' which is currently unchecked.
- Idle Timeout:** Shows 'Disconnect after' set to 60 min. of inactivity via a dropdown menu.

Figure 16 Security Settings

The Security Settings fields:

Account Blocking – decide on the number of attempts to login with a wrong username or password after which there is a time lock or a total block.

Password Policy – You have the option of a standard or high security level of password. The table below shows the parameters of the 2 options.

Standard security policy	High security policy
6 characters or more	8 characters or more must include at least 1 digit and 1 upper case letter and 1 “special” character as follows !@#\$%^&*()_+=[]”’;?/><
Must not include the user name	Must not include the user name

Check the box to enable the high security password policy. Unchecked, the standard security policy applies.

Idle Timeout – Select the Timeout inactivity period after which the user is disconnected from the system. Choose **No Timeout** to disable Timeout.

Click **Save & Restart** to save any configuration changes done to the **Security Settings** page. The Smart 116 IP system restarts with the new changes.

19. Security > SSL Certificate

You can install an SSL certificate.

To do so:

From the menu, select **SSL Certificate**, the install SSL Certificate page appears, see Figure 17.

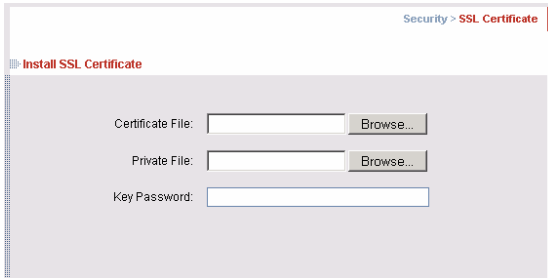


Figure 17 Install SSL Certificate page

Certificate File - Browse to locate the **cer** file.

Private File - Browse to locate the **private key** file.

Key Password - Type the “private key” password.

Click **Save & Restart**.

20. Maintenance > Firmware Upgrade

Upgrade the Smart 116 IP firmware to take advantage of new features. Download the firmware from the Support section of Minicom’s website –www.minicom.com. Save the firmware file on the Client computer.

From the menu select **Firmware Upgrade**. The Firmware Upgrade window appears showing the current firmware version see Figure 18.



Figure 18 Firmware Upgrade

1. Locate and upload the firmware file.
2. Verify the current and uploaded version of the firmware.
3. Click **Start Upgrade**. The upgrade starts. On completion, click **Reboot**. The unit reboots. After about 30 seconds the Login page appears.

Note!

Depending on the type of firmware upgrade, the following settings may be erased: User settings, server names, mouse and video adjustments. For more information refer to the firmware release notes.

The network settings remain intact.

21. Restore Factory Settings

You can restore the Smart 116 IP unit to the factory settings. This restores the original Smart 116 IP parameters, resetting all the information added by the administrators, including: Network settings*, Servers, Switches, Users, Passwords etc.

* You have the option to preserve Network settings – explained below.

Warning! Once reset the data cannot be retrieved.

To restore factory settings:

1. From the menu select **Restore Factory Settings**. Restore Factory Settings appears see Figure 19.

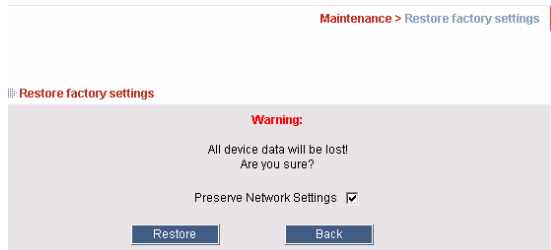


Figure 19 Restore factory settings

2. Check the box if you want to preserve Network settings.
3. Click **Restore**.

22. Logging out

To exit the Configuration menu and close the session, click **Logout**.

Only one Administrator can log into the Configuration area at a time. An idle timeout of 30 minutes terminates the session.

23. Starting a remote session

At a Client computer open Internet Explorer (6.0 and above) and type the Smart 116 IP's IP address. <https://IP address>. (Note! Only SSL connections are allowed, therefore type HTTPS before the IP address or the name of the Smart 116 IP). The Login page appears. Type your username and password and press Enter. By default, the user name is: **admin** and the password is **access**, (both lower case).

On first connection install the Minicom certificate and ActiveX control. You must login as an Administrator to your computer to install the ActiveX control. Once the ActiveX control is installed, all types of users can login.

On connecting, the screen of the lowest numbered Target Server that the user has permission to access appears. Figure 20 illustrates the remote session window.

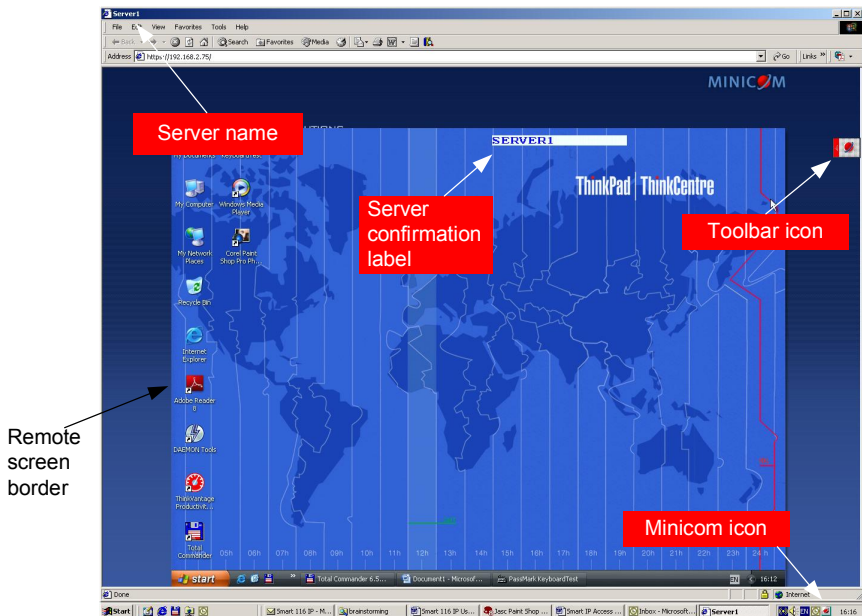


Figure 20 Remote console window

On the remote console you have the following:

Server Confirmation label – This confirms the identity of the current server accessed and disappears by default after 30 seconds, (this period can be adjusted in the OSD – explained in Section II of the guide). It appears again when switching to a different server. The currently accessed server identity can be checked any time by looking at the **Server name** on the Internet Explorer title bar.

Toolbar icon – This is the minimized toolbar from which you switch and configure the system.

Minicom icon – Hold the mouse over the icon to view information about current server, connection time and video mode.

23.1 Taking over a busy remote session

While only one user can have control, many users can be connected simultaneously. When connecting to a busy Target Server an Administrator has the option to take over the Target Server. A User only has this option when the current session is run by another User, but not by an Administrator. The following message appears



Figure 21 Busy remote session options

Choose to Take Over or View Only or Cancel.

When watching a screen in View Only mode you can Double click inside the Remote screen border – see Figure 20 – to take over the remote control. The current user sees a message stating that control has been taken over.

23.2 Full screen mode

Work on the Target Server as if you are working on a local computer, with full screen mode.

To work in full screen mode:

1. Ensure that the Client computer has the same screen resolution as the Target Server.
2. Press **F11**. The Internet Explorer window disappears, leaving the Internet Explorer menu bar at the top.
3. Right click the Internet Explorer menu bar and check Auto-Hide. The Internet Explorer menu bar disappears. You are in full screen mode.

To exit full screen mode:


Press **F11**. Or place the mouse at the top of the window to display the Internet Explorer toolbar and click the Restore button.

Note! Full screen mode can also be activated from the Toolbar menu, see page 33.

23.3 The Toolbar


To maximize the Toolbar:




Click the arrow . Click again to minimize the Toolbar.

When maximized, the Toolbar can be dragged and dropped to anywhere on the



screen, by dragging the icon . When minimized the icon glides to a side of the screen.

To hide the Toolbar, either:

Double-click the Smart 116 IP System tray icon .

Or



Press **F9**.

To display the Toolbar repeat the above action. See also page 33.

23.4 Switching to a different server

To connect to a different server:




1. From the Toolbar, click , or right-click . A list of available servers appears. The currently connected server is highlighted in bold.
2. Click the desired server name. The screen of the selected server appears.

23.5 Changing the performance settings

You can alter the bandwidth settings from the Toolbar.

To alter the settings:



From the Toolbar, click . The Settings.. Dialog box appears, see Figure 22.

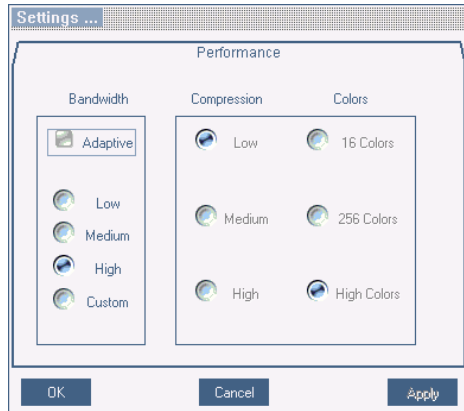


Figure 22 Settings.. Dialog box

Bandwidth

Choose from the following options

Adaptive – automatically adapts to the best compression and colors according to the network conditions. (Not recommended because network parameters may change frequently impacting on user experience).

Low - Select Low for high compression and 16 colors.

Medium - Select medium for medium compression and 256 colors. Medium is recommended when using a standard internet connection.

High - For optimal performance when working on a LAN, select High. This gives a low compression and high colors (16bit).

Custom – You can choose your own compression and color levels.

Click **OK**. The screen of the last accessed Target Server appears.

23.6 Adjusting the Video settings

To change the video settings:

From the Toolbar, click . You have the following options:

- Refresh
- Manual Video Adjust
- Auto Video Adjust

Each option is explained below.

23.6.1 Refresh

Select Refresh or press **Ctrl+R** to refresh the Video image. Refresh may be needed when changing the display attributes of a Target Server.

23.6.2 Manual Video Adjust

Use the manual video adjustment for fine-tuning the Target Server video settings after auto adjustment or for adapting to a noisy environment or a non-standard VGA signal or when in full-screen DOS/CLI mode.

To adjust the video manually:

Click Manual Video Adjust. The manual controls appear, see Figure 23. Also a red frame appears around the screen. This represents the screen area according to the Server's screen resolution. Perform the adjustments inside and relative to this frame.

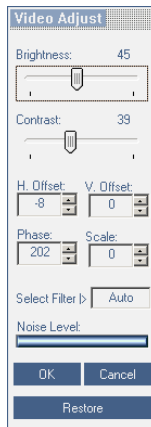


Figure 23 Manual Video Adjustments controls

Brightness / Contrast - use the scales to adjust the brightness and contrast of the displayed image. Move the sliders to change the displayed image. Click in the area of the sliders for fine-tuning.

For the following controls choose the appropriate measurement.

Horizontal Offset - defines the starting position of each line on the displayed image.

Vertical Offset - defines the vertical starting position of the displayed image.

Phase - defines the point at which each pixel is sampled.

Scale – defines the scale resolution of the session image.

Select Filter - defines the filter of the input video from the server. A higher filter reduces the noise level but makes the image heavier.

Noise Level - represents the Video "noise" when a static screen is displayed.

23.6.3 Auto Video Adjust

To adjust the video automatically:

Click **Auto Video Adjust**. The process takes a few seconds. If the process runs for more than 3 times, there is an abnormal noise level. Check the video cable and verify that no dynamic video application is running on the Target Server's desktop.

Perform the procedure where necessary for each Target Server or new screen resolution.

23.7 Power cycle



This button is for future Serial power management options.

23.8 Keyboard key sequences



Click . A list of defined keyboard sequences appears. When clicked, these transmit directly to the Target Server, and will not affect the Client computer.

For example, select **Ctrl-Alt-Del** to send this three key sequence to the Target Server to initiate its Shutdown/Login process.

To add a keyboard sequence:

Click **Add/Remove**. The Special Key Manager box appears see Figure 24.

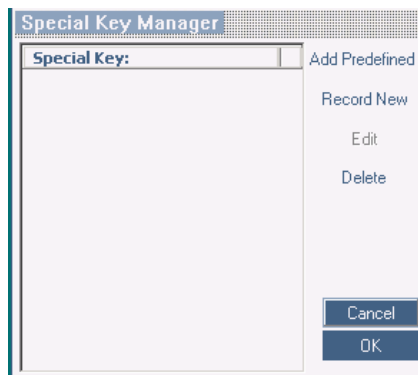


Figure 24 Special Key Manager box

To add a predefined sequence:

1. Click Add Predefined. A list of sequences appears.
2. Select the desired sequence and click OK. The sequence appears in the Special Key Manager box.
3. Click OK. The sequence appears in the Keyboard Key sequence list.

To record a key sequence:

1. From the Special Key Manager box press **Record New**. The Add Special Key Dialog box appears, see Figure 25.

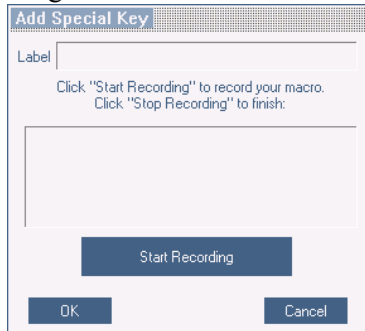


Figure 25 Add Special Key Dialog box

2. Give the key sequence a name in the Label field.
3. Click **Start Recording**.
4. Press the desired keys. The key sequence appear in the area provided.
5. Click **Stop Recording**.
6. Click **OK**.

To edit a key sequence:

1. From the Special Key Manager Dialog box select the desired key.
2. Click **Edit**.
3. Click **Start Recording**
4. Press the desired keys. The keys appear in the area provided.
5. Click **Stop Recording**.
6. Click **OK**.

23.9 Synchronizing mouse pointers

When working at the Client computer, two mouse pointers appear: The Client computer's is on top of the Target Server's. The mouse pointers should be synchronized. The following explains what to do if they are not synchronized.


Warning

Before synchronizing mouse pointers adjust the video of the Target Server, (explained above) otherwise mouse synchronization may not work.

23.9.1 Aligning the mice pointers

When accessing the Target Server, the mice may appear at a distance to each other.


To align the mouse pointers:

From the Toolbar click  / **Align** or press **Ctrl+M** simultaneously. The mice align.

23.9.2 Calibrating mice pointers

A Target Server may have a different mouse pointer speed to the Client computer. Calibrating automatically discovers the mouse speed of the Target Server and aligns the two pointers.

To perform the calibration when the Target Server Operating system is, Windows NT4, 2000 or 98:

From the Toolbar click  / **Calibrate**. Smart 116 IP saves this alignment so calibration is only needed once per Target Server.

If the Video Noise Level is above zero, calibration may not work. Go to Video Adjustment and try to eliminate the noise by pressing Auto video adjust and/or adjusting the bars in Manual video adjust, then perform the mouse calibration.

Note! If the mouse settings on the Target Server were ever changed, you must synchronize mouse pointers manually, as explained below.

23.9.3 Manual mice synchronization

If the mouse settings on the Target Server were ever changed, or when the Operating system on the Target Server is, Windows XP / 2003 Server / Vista, Linux, Novell, SCO UNIX or SUN Solaris you must synchronize the mouse pointers manually.

To manually synchronize mouse pointers:

1. From the Toolbar click  / **Manual Settings**. The **Mouse Settings** Dialog box appears see Figure 26.

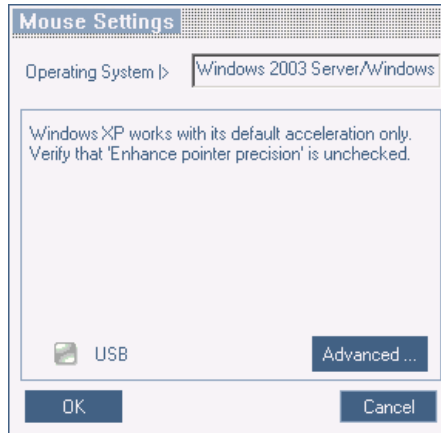



Figure 26 Mouse Settings Dialog box

2. Select the Target Server's Operating System and click OK. Instructions and sliders appear.
3. Follow the instructions and set any relevant sliders to the same values as set in the Target Server's Mouse Properties window.

2 examples!

For Windows XP, 2003 Server, Vista and Longhorn Server. Go to the Mouse settings on the Target Server and uncheck Enhance pointer precision.

For Windows NT4, 98, ME, 2000. If Mouse Properties were ever changed for the Target Server – even if they have been returned to their original state - uncheck default -  Default .

Click **OK**. The mouse pointers should be synchronized.

23.9.3.1 USB

The USB option in Mouse Settings box is available for RoC and RICC USB, for unsupported operating systems and SUN Solaris. Use this option if you are sure of the custom acceleration algorithm you are using, or have been informed so by customer support.

23.9.3.2 Advanced – Mouse Emulation

In the Advanced Mouse settings, you can set the type of mouse connected to Smart 116 IP's local console.


Click  the Mouse Emulation Dialog box appears, see Figure 27.



Figure 27 Mouse Emulation Dialog box

Select the mouse connected to the Local Console port on the Smart 116 IP, e.g. if the local mouse is a 2 button mouse, select **Standard Mouse**.

Switch Acceleration - This setting should **NOT** be changed.

Max Rate - this defines the maximum mouse report rate. For Sun Solaris the default value is 20 in order to support older Sun versions.

23.10 Minicom icon menu features



Right-click the Minicom icon, a menu appears. From this menu you can access the connected devices. You also have the following features:

Disconnect – You can disconnect the session by clicking Disconnect.

About - Click About to verify the Client, Firmware, KME (Keyboard/Mouse Emulation firmware) and Switch file versions installed on your Smart 116 IP.

Local Settings – Click Local settings, the Client Configuration Dialog box appears, see Figure 28

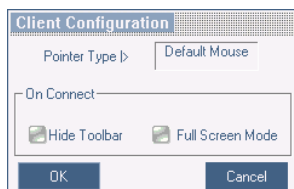



Figure 28 Client Configuration Dialog box

Pointer type – From the Drop-down menu you can change the Client computer mouse pointer to appear as a dot or to not appear at all.


Hide Toolbar – Check this option to hide the Toolbar from the next reconnection onwards. To toggle the Toolbar on and off, press **F9** or double-click the System tray icon . See above page 25.

Full Screen Mode - Check this option to make the remote session screen appear in full screen mode from the next reconnection onwards. To toggle the full screen mode on and off, press **F11**.

Configuration – This only appears in the menu when an Administrator is logged in. Click **Configuration** to access the Web configuration interface.

23.11 Disconnecting the remote session



To disconnect the session, on the Toolbar, click . The Login page appears. You can re-login, or close the browser window to disconnect the session.

24. Troubleshooting - Safe mode

From the Safe mode you can:

Restore factory defaults - When you cannot access the system e.g. you have forgotten the Username or Password, restore factory defaults from the Safe mode. (Section 21 on page 22 explained how to restore factory settings from the Web interface).

Restore the device firmware – If during a firmware update there is a power failure and you can no longer access the system you can restore the device firmware from the Safe mode.

24.1 Entering Safe mode

To enter Safe mode:

1. Press and hold down the **Local** button for 3-4 seconds and at the same time power up the Smart 116 IP. The device boots up in Safe mode.
2. Wait until the unit finishes booting (1-2 minutes).
3. You need to know the IP address of the Smart 116 IP. The IP address depends on whether there is a DHCP server on the network. If there is, the DHCP server assigns an IP address to the Smart 116 IP. If there is no DHCP server, the unit boots with the static IP address 192.168.2.155.

Open Internet Explorer and type the following into the Address box: [http://IP address/config](http://IP_address/config). (Do not start the address with **https**). The Login page appears, see Figure 29.

The image shows a web browser window with a login form. At the bottom left, there are two input fields. The first is labeled 'User:' and the second is labeled 'Password:'. To the right of the 'Password:' field is a 'Login' button.

Figure 29 Login page

4. Type username: **admin** , password: **SAFEmode**. (Case sensitive). (This username and password works only in Safe mode). A menu appears, see Figure 30.

The image shows a web browser window displaying the 'Maintenance > Firmware Upgrade' menu. On the left, there are two blue links: 'Firmware Upgrade' and 'Restore Factory Settings'. Below these links are two buttons: 'Logout' and 'Restart'. In the center, there is an 'Upload File:' label followed by a text input field and a 'Browse...' button.

Figure 30 Safe mode menu

24.2 Restoring factory defaults

To restore factory defaults:

1. From the menu choose **Restore Factory Settings**. A warning appears see Figure 31.

The image shows a warning dialog box. At the top, it says 'Warning:' in red. Below that, the text reads: 'All device data will be lost! Are you sure?'. At the bottom, there are two buttons: 'Restore' and 'Back'.

Figure 31 Warning

2. Click **Restore**. A further warning appears, see below.

**Figure 32 Warning**

3. Click **OK**, the factory defaults are restored. When the process finishes Figure 33 appears.

**Figure 33 Reboot**

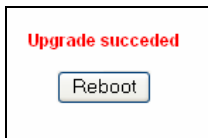
4. Click **Reboot** to restart the unit.

24.3 Restoring the device firmware

Contact Minicom Technical Support support@minicom.com, to receive the Upgrade firmware required to restore the device firmware. Save the Upgrade firmware on the hard disk of a computer connected to the network.

To restore the device firmware:

1. From the Safe mode menu choose Firmware Upgrade.
2. Locate the Upgrade firmware and click Install, then click Start Upgrade. The firmware upgrades. When the process finishes Figure 34 appears.

**Figure 34 Reboot**

3. Click **Reboot** to restart the unit.

Section II

Section II explains how to operate the Smart 116 IP Switching system locally (sections 25 and 26) and how to upgrade the Smart 116 IP firmware (section 27). Section 28 deals with troubleshooting.

25. Switching between computers

Switch between the connected computers by either:

- Keyboard hotkeys
- The OSD (On Screen Display)

25.1 The keyboard hotkeys

To switch to the next computer forwards press **Shift** then, +. Release **Shift**, before pressing +.

To switch to the next computer backwards press **Shift** then, -. Release **Shift**, before pressing -.

Note! With a US English keyboard you can use the + key of the alphanumeric section or of the numeric keypad. With a Non-US English keyboard only use the + key of the numeric keypad.

26. The OSD

To display the OSD:

1. Ensure there is no remote user connected. To disconnect the remote user press the **Local** button on the Smart 116 IP.
2. Press **Shift** twice. The OSD Main window appears. See Figure 35. Lines with yellow text show active computers. Lines with blue text show inactive computers. The Type column indicates a computer “C” is connected to the port.

MINICOM		SMART 116 IP MAIN	
Port number	NAME	TYPE	
01	SERVER1	C	
02	SERVER2	C	
03	SERVER3	C	
04	SERVER4	C	
05	SERVER5	C	
06	SERVER6	C	
07	SERVER7	C	
08	SERVER8	C	
F1-HELP		F2-SETTINGS	

Port number appears here →

Instruction keys →

C=computer

Figure 35 OSD Main window

26.1 Navigating the OSD

To navigate up and down use the Up and Down arrow keys.

To jump from one column to the next (when relevant) use the Tab key.

To exit the OSD or return to a previous window within the OSD press **Esc**.

26.2 Selecting a computer

To select a computer:

1. Navigate to the desired computer line.

Or, type the port number of the desired computer.

2. Press **Enter**. The selected computer is accessed. A Confirmation label appears showing which computer is accessed.

Note! When the OSD is displayed you cannot select computers using the keyboard hotkeys.

26.3 The OSD settings - F2

Press **F2**. The OSD Settings window appears see Figure 36.

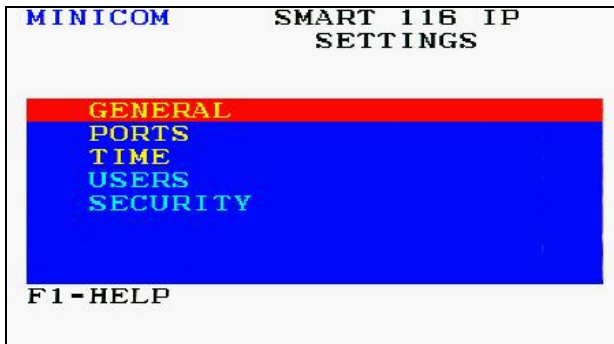


Figure 36 Settings window

Note! When the OSD is password protected (explained below) only the Administrator has access to the F2 settings window.

26.3.1 The General settings

With the red line on the word **GENERAL**, press **Enter**. The General settings window appears see Figure 37.

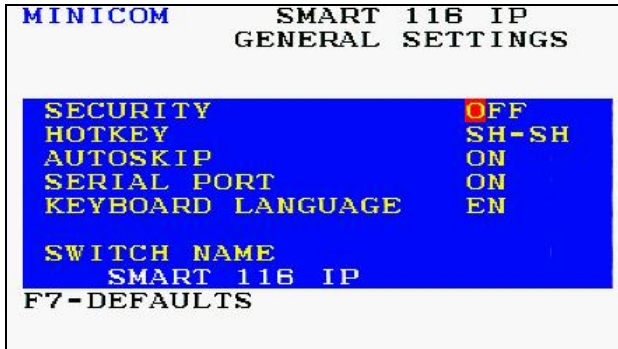


Figure 37 General Settings window

From this window you can do the following:

26.3.1.1 Security

The OSD comes with an advanced password security system that contains 3 different security levels. Each security level has different access rights to the system.

These levels are as follows:

Administrator (Status A)

The Administrator can:

- Set and modify all Passwords and security profiles
- Fully access any computer
- Use all OSD functions

Supervisor (Status S)

The Supervisor can:

- Fully access any computer
- Access the following OSD functions only –F4 Scan, F5 Tune and F6 Moving the Confirmation label.

User (Status U)

There are 6 different Users in the Smart 116 IP system. Each User has a Profile set by the Administrator that defines the access level to different computers. There are 3 different access levels - explained on page 42.

26.3.1.2 Activating password protection

By default OSD access is not password protected. Only the Administrator can password-protect the OSD or disable password protection.

To do so:

1. In the General settings window navigate to the Security line.
2. Press the Space bar to toggle between Security On and Off. The password box appears.
3. Type the Administrator's password (default is "admin").
4. Press **Enter**. The new security status is set.

26.3.1.3 Changing the OSD hotkey

By pressing **Shift**, **Shift** the OSD appears. You can replace **Shift**, **Shift** with any of the following:

- Ctrl, Ctrl
- Ctrl, F11
- Print Screen

To change the hotkey:

1. Navigate to the Hotkey line.
2. Press the Space bar to toggle between options. To display the OSD in future press the new hotkey.

26.3.1.4 Autoskip

With the Autoskip feature, the arrow keys only access the active computer lines on the OSD. When Autoskip is Off, The arrow keys access both active and inactive computer lines.

To change the Autoskip setting:

1. Navigate to the Autoskip line.
2. Toggle between the options using the Space bar.

26.3.1.5 Serial port

This option is disabled in Smart 116 IP. Leave this option on its default setting ON.

26.3.1.6 Changing the Keyboard language

The keyboard is preset to US English, this can be changed to French (FR) or German (DE), as follows:

1. Navigate to the Keyboard language line.
2. Toggle between the options using the Space bar.

26.3.1.7 Editing the Switch name

You can substitute up to 18 characters in the line. A space constitutes a character. When there is more than one switch in the system give each Switch's OSD a different name.

26.4 F7 Defaults

Press F7 to return the OSD to the factory default settings. **Note!** All changes made will be erased.

26.5 The Ports settings

In the Settings window navigate to the Ports line and press **Enter**. The Ports settings window appears see Figure 38.

MINICOM		SMART 116 IP PORTS SETTINGS	
	NAME	KB	HKEY
01	SERVER1	PS	NO
02	SERVER2	PS	NO
03	SERVER3	PS	NO
04	SERVER4	PS	NO
05	SERVER5	PS	NO
06	SERVER6	PS	NO
07	SERVER7	PS	NO
08	SERVER8	PS	NO

Figure 38 Ports Settings window

26.5.1 Editing the computer name

In this window you can edit the computer names with up to 15 characters. (To avoid confusion the names given in the OSD should match the names given in the web configuration).

To erase a character:

Select it and press the **Space bar**. Blank spaces remain in place of the erased character.

To erase an entire line:

Place the cursor at the beginning of the line. Keep the **Space bar** depressed until the line is erased.

26.5.2 Keyboard (KB)

The Smart 116 IP operates with Windows, Linux, HP UX, Alpha UNIX SGI, DOS, Novell, MAC-USB or Open VMS.

By default the keyboard mode is set to PS for Intel based computers.

For the other systems set the KB column as follows:

- U1 for HP UX
- U2 for Alpha UNIX, SGI, Open VMS
- U3 for IBM AIX

To change the setting:

1. On the desired line, press Tab to jump to the KB column.
2. Toggle between the options using the Space bar.

26.5.3 Adding/changing a hotkey (HKEY)

Cascade the Smart 116 IP by connecting another Smart Switch to a Computer port instead of a computer, and then connecting more RICCs to the second Switch.

You must define a different hotkey for the OSD of each Switch. The hotkeys can be any of the choices as set out above on page 39. Use the hotkey when you select the Switch's port in the first level OSD – the second level's OSD then appears.

To add/change a hotkey:

1. On the line to which the Switch is connected, press Tab to jump to the HKEY column.
2. Toggle between the options using the Space bar.

26.6 The Time settings

In the Settings window navigate to the Time line and press **Enter**. The Time settings window appears see Figure 39.

MINICOM		SMART 116 IP TIME SETTINGS		
	NAME	SCN	LBL	T/O
01	SERVER1	030	030	030
02	SERVER2	030	030	030
03	SERVER3	030	030	030
04	SERVER4	030	030	030
05	SERVER5	030	030	030
06	SERVER6	030	030	030
07	SERVER7	030	030	030
08	SERVER8	030	030	030

Figure 39 Time settings window

26.6.1 Scan (SCN) - Label (LBL) - Time out (T/O)

SCN - In the **SCN** column, change the scan period.

LBL - In the **LBL** column, change the display period of the Confirmation label showing which computer is currently accessed.

T/O - When password protection is activated you can automatically disable the Management keyboard, mouse and screen after a preset time of non-use. Set this Timeout period in the **T/O** column.

To set the above periods:

1. On the desired line press Tab to jump to the desired column.
2. Place the cursor over one of the 3 digits and type a new number. Enter a leading zero where necessary. For example, type 040 for 40 seconds.

Typing 999 in the **LBL** column displays the label continuously. Typing 000 – the label will not appear.

Typing 999 in the **T/O** column disables the Timeout function. Typing 000 – the Timeout function works immediately.

Typing 999 in the **SCN** column displays the screen for 999 seconds. Typing 000 – the computer screen is skipped.

26.7 Users

In the Settings window navigate to the Users line and press **Enter**. (Note! Users is only enabled if the security status is set to On, see page 39). The Users settings window appears see Figure 40.

MINICOM		SMART 116 IP	
		USERS	SETTINGS
		USER	
		123456	
NAME			
01	SERVER1	Y	YYYYYY
02	SERVER2	Y	YYYYYY
03	SERVER3	Y	YYYYYY
04	SERVER4	Y	YYYYYY
05	SERVER5	Y	YYYYYY
06	SERVER6	Y	YYYYYY
07	SERVER7	Y	YYYYYY
08	SERVER8	Y	YYYYYY

Figure 40 Users settings window

There are 3 different access levels. These are:

- Y – Full access to a particular computer.
- V – Viewing access only, to a particular computer (No keyboard/mouse functionality)
- N – No access to a particular computer – A TIMEOUT label appears if access is attempted

To give each user the desired access level:

1. Navigate to the desired computer line and User column.
2. Toggle between the options using the Space bar.

26.8 Security

In the Settings window navigate to the Security line and press **Enter**. (Note! Security is only enabled if the security status is set to On, see page 39). The Security settings window appears see Figure 41.

MINICOM SMART 118 IP SECURITY SETTINGS		
-----NAME-----	PASSWORD	T
ADMINISTRATOR	ADMIN	A
SUPERVISOR	SUPER	S
USER1	USER1	U
USER2	USER2	U
USER3	USER3	U
USER4	USER4	U
USER5	USER5	U
USER6	USER6	U

Figure 41 Security settings window

The 'T' column on the right hand side stands for Type of access permission.

There can only be 1 Administrator password, 1 Supervisor password, and 6 User passwords.

To change a user name or password:

1. Navigate to the desired line and column.
2. Type a new user name / password. User authentication is done solely via the password there is no security significance to the names.

By default the User Profile settings are full access.

26.9 The OSD HELP window – F1

To access the HELP window press F1. The HELP window appears see Figure 42.

MINICOM SMART 118 IP HELP	
SCAN	F4
TUNE	F5
MOVE LABEL	F6
NEW MONITOR-DDC2	F10
MOVE UP-DOWN	▲ ▼
SELECT COMPUTER	ENTER
CHOOSE OPTION	SPACE
NEXT COLUMN	TAB
EXIT	ESC

Figure 42 HELP window

Please note!

All the functions set out in the Help window are performed from the Main window. The Help window is merely a reminder of the hotkeys and their functions.

26.10 Scanning computers – F4

Where necessary adjust the scan time in the Time Settings window, see above.

To activate scanning:

1. Press **Shift** twice to open the OSD.
2. Press **F4**. Your screen displays each active computer sequentially, with the Scan label appearing in the top left corner.

To deactivate scanning:

Press **F4**.

26.11 Tuning – F5

You can tune the image of any computer screen from the Select Computer window.

To adjust the screen image:

1. Navigate to the computer you wish to adjust.
2. Press **F5**. The screen image of the selected computer appears, together with the Image Tuning label.
3. Adjust the image by using the **Right** and **Left** Arrow keys.
4. When the image is satisfactory, press **Esc**.

Note! Picture quality is relative to distance. The further away a remote computer is from the Smart 116 IP, the lower the image quality, and the more tuning needed. So place the higher resolution computers closer to the Switch.

26.12 Moving the label – F6

Position the Confirmation label anywhere on the screen.

To position the label from the Main window:

1. Navigate to the desired computer using the **Up** and **Down** arrow keys.
2. Press **F6**. The selected screen image and Identification label will appear.
3. Use the arrow keys to move the label to the desired position.
4. Press **Esc** to save and exit.

27. Upgrading the Smart 116 IP firmware

With the Smart 116 IP Switch Update software you can upgrade the firmware for the:

- Switch processors
- RoC/RICCs

The Update software enables you to add new features and fix bugs in a quick and efficient manner. Install the Update software on any computer, even one not part of the Smart 116 IP system.

The software can be downloaded from the Support section at www.minicom.com, it is also on the supplied CD.

For newer versions of the Update software or firmware for the Switch and RoC/RICCs go to the Support section at www.minicom.com.

27.1 System requirements for the Update software

- Pentium 166 or higher with 16 MB RAM and 10 MB free Hard Drive space.
- Free Serial port.
- Windows 2000, XP or Windows 2003 Server.

27.2 Connecting the Smart 116 IP System

To update the firmware the Smart 116 IP system must be connected and switched on.

27.3 Connecting the RS232 Download cable

To run the Update software, connect the RS232 Download cable (p/n 5CB40419) to the computer containing the software, and to the Smart 116 IP Switch Flash port see Figure 43.

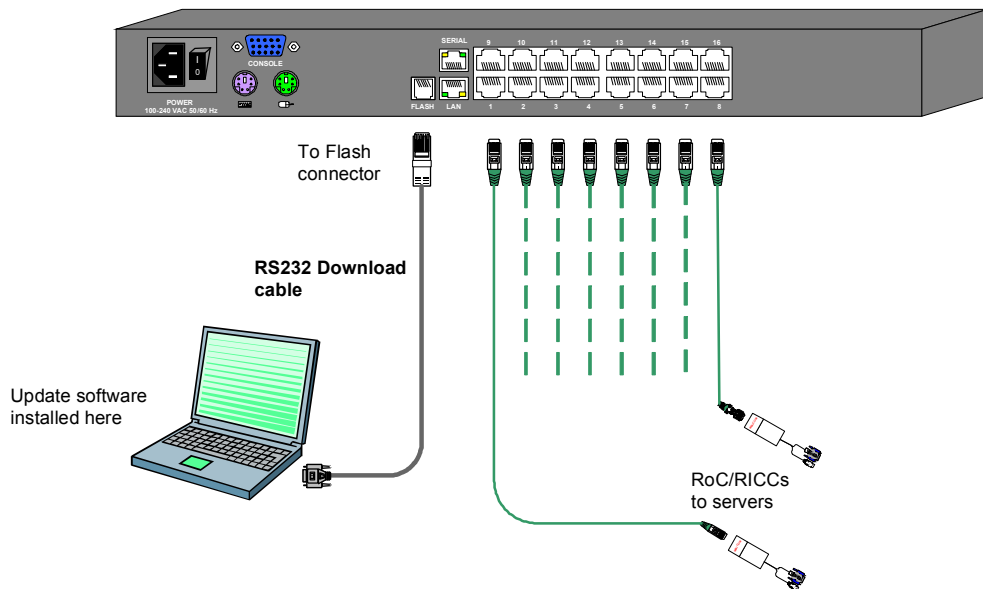


Figure 43 RS232 cable

27.4 Installing the software

To install the Update software:

1. Download the software from the Support section of Minicom's website, or locate it on the supplied CD.
2. Install the software on the computer's hard drive.

27.5 Starting and configuring the Update software

1. Select Start/Programs/Smart 116 IP Switch Update/Smart 116 IP Switch



Update or click the shortcut icon on the Desktop. The Smart 116 IP Switch Update window appears. See the figure below.

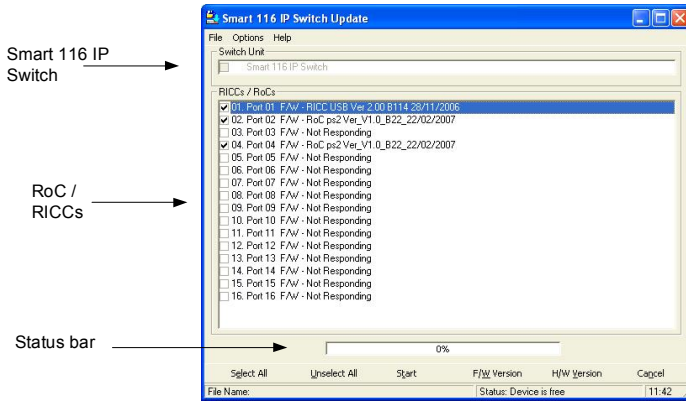


Figure 44 Smart 116 IP Switch Update window

The table below explains the functions of the buttons and boxes in the Update window.

Button or Box	Function
Select All	Selects all RoC/RICCs
Unselect All	Unselects selected RoC/RICCs
Start	Starts firmware download
F/W Version	Displays the firmware version numbers
H/W Version	Displays the hardware version numbers
Cancel	Cancels selected function
10:06	System time
Status:	Displays download status
File Name:	Name of Update file

- To change the Com Port from the Options menu choose Com Port. The Com Port Dialog box appears. See Figure 45.

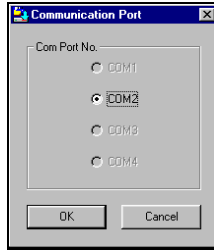


Figure 45 Com Port Dialog box

3. Choose the Com Port the RS232 Serial cable is connected to and click OK.

27.6 Verifying the version numbers

Before upgrading the firmware, you must first verify which firmware and hardware versions you have.

27.6.1 116 IP Switch version

To verify the Smart 116 IP Switch version:

1. Select the 116 IP Switch checkbox.
2. Click **F/W Version**. The firmware versions of the Translator, Master and OSD appear, see Figure 46.

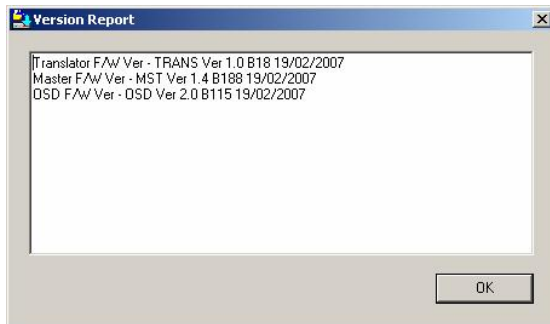


Figure 46 Firmware version report

3. Click **H/W Version**. The hardware version of the Translator appears, see Figure 47.

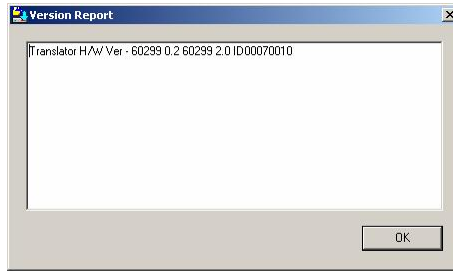


Figure 47 Hardware version report

27.6.2 RoC/RICC version number

Before you can tick a RoC/RICC, you must unselect the 116 IP Switch checkbox.

To verify the RoC/RICC version number:

1. Check one or more or all of the RoC/RICCs.
2. Click **F/WVersion**. The firmware version number appears.
3. Click **H/WVersion**. The hardware version number appears.

When “**Not responding**” appears, there is no computer connected, or it is switched off.

27.7 Obtaining new firmware

Download the latest firmware for your system from www.minicom.com

27.7.1 Updating the firmware

Warning!

Never switch off any computer connected to the Smart 116 IP system during the updating process.

To update the firmware:

1. Select the option to update 116 IP Manager or the RoC/RICCs.
2. From the **File** menu, choose **Open**. The **Open** box appears. See Figure 48.
3. Navigate to the folder that contains the firmware update file. You may only see the files that match the file selection mask.

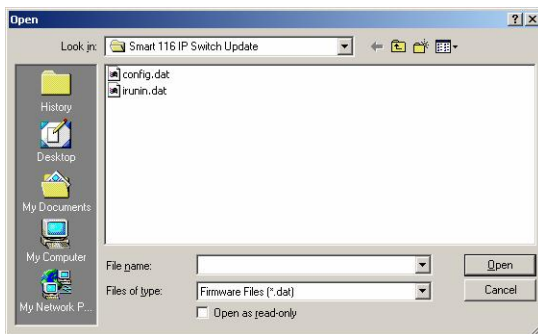


Figure 48 Open box

4. Open the file.
5. Click **Start**. The Smart 116 IP Switch Update flashes the firmware. On completion the firmware version number appears.
6. Check that the updated version number is correct by pressing F/WVersion.

Firmware Update generates one log file per session that displays a chronological list of actions. You can read the log file in any ASCII text editor. The log file is located in the Windows directory.

28. Update software - Troubleshooting

This section covers:

- Resetting the units
- Returning the OSD to the factory default settings
- Getting the current status
- Communication Error message
- Electricity failure

28.1 Resetting the Smart 116 IP or RoC/RICCs

Reset the Smart 116 IP Switch or RoCs/RICCs when for example the unit hangs or when the mouse fails to work properly. Resetting is done via the Flash port, and avoids the need to shut down the computers.

NOTE! The Reset function does not affect the parameters of the unit settings.

To reset the Smart 116 IP or RoC/RICC units:

1. For the Smart 116 IP, select the 116 IP Switch checkbox.

For the RoC/RICCs, check one or more RoC/RICCs.

2. Select Options/Advanced/Reset. The unit resets. The system should now be operational.

28.2 Setting default values for the OSD

To return the OSD to the factory default settings:

Select Options/Advanced/Set Default. A warning appears, click OK. The OSD returns to the factory default settings.

28.3 Get Status

If there is a break in communication between the Update software and the system, select Options/Get Status to get the current status of the computers in system.

28.4 Communication Error message

When updating a unit and a Communication Error message appears, do the following:

1. Check that the RS232 Serial cable's RS232 connector is connected to the Switch's Flash port.
2. Check that the RS232 Serial cable's DB9F connector is connected to the laptop's Serial port.
3. Verify there is no Remote session in progress by pressing the Local button.
4. Restart the update process.

28.5 Electricity failure

When the electricity fails while updating the Smart 116 IP firmware, do the following:

If the electricity fails during the firmware update of the Switch, a **Communication Error** message appears. Simply resume the firmware update by opening the folder that contains the firmware update file and continue from there.

If the electricity fails during the firmware update of the RICC's a **Not Responding** or **Upgrade Error** message appears. Restart the upgrade from the beginning.

(For electricity failure during a firmware upgrade of the digital part of the Smart 116 IP, see page 33).

29. Technical specifications

Operating systems	Target Server Windows, Linux, UNIX and other major operating systems Client Computer Windows 2000 or higher with IE 6.0 or higher and ActiveX
Resolution	Target Server Up to 1600 x 1200 @ 85Hz Client Computer Recommended - resolution should be higher than on Target Server
Video and mouse synchronization	Both auto and manual modes
Security	128-bit SSL encryption
Connections	Ethernet – RJ45 – 10/100 Mbit/sec autosensing Serial – RJ45 Local KVM connection – Screen HDD15, Keyboard./Mouse – MiniDIN6 Flash – RJ11 Server – RJ45
Weight	2.54Kg / 5.6lbs
Dimensions (H x D x W)	44x 220 x 431 mm / 1.6 x 6.93 x 17"
Power input	100 – 240 VAC 50 / 60 Hz
Operating temperature	0°C to 40°C / 32° to 104°F
Storage temperature	-40°C to 70°C / -40°F to 158°F
Humidity	80% non condensing relative humidity

30. Video resolution and refresh rates

Hz →	56	60	65	66	70	72	73	75	76	85	86
640x480		x		x	x	x		x		x	
720x400					x					x	
800x600	x	x				x		x		x	x
1024x768		x			x	x	x	x	x	x	
1152x864								x			
1152x900				x					x		
1280x720		x									
1280x768		x						x			
1280x960		x								x	
1280x1024		x				x		x	x	x	
1600x1200		x	x		x			x		x	

31. Safety

The device must only be opened by an authorized Minicom technician. Disconnect device from AC mains before service operation!

32. User guide feedback

Your feedback is very important to help us improve our documentation. Please email any comments to: ug.comments@minicom.com

Please include the following information: Guide name, part number and version number (as appears on the front cover).

Regional Offices

Germany

Kiel

Tel: + 49 431 668 7933

info.germany@minicom.com

France

Vincennes

Tel: + 33 1 49 57 00 00

info.france@minicom.com

Italy

Rome

Tel: + 39 06 8209 7902

info.italy@minicom.com

England

Camberley

Tel: + 44 (0) 1276 25053

info.uk@minicom.com

www.minicom.com

